KOMMANDEUR [illegible] DNA 1)

AT REVIN, FRANCE, JUNE 1945

The "Report on Interrogation etc." will be issued in parts as completed. The parts will be numbered as follows:

TICOM/I-19b - Report on Interrogation

TICOM/I-19c - Report on Interrogation, Annexe 1 (Text)

TICOM/I-19d - Report on Interrogation, Annexe 1 (Figs.)

TICOM/I-19e - Report on Interrogation, Annexe 1 (Models)

TICOM/I-19f - Report on Interrogation, Annexe 2

TICOM/I-19g - Report on Interrogation, Annexe 3

Annexe 1 (TICOM/I-19c, d, e) deals with cryptanalysis of Russian ciphers; Annexe 2 (TICOM/I-19f) with traffic analysis of Russian wireless traffics; Annexe 3 (TICOM/I-19g) with German Army (Eastern Front) Sigint organisation and method.

Distribution will be identical for TICOM/I-19a-g

Issued simultaneously with TICOM/I-19a

TICOM/I-19c and 19d.

TICOM
29 June 1945

Copy No. 16
No. of pages 1

Distribution:

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt.Col. Leathem

U.S.
26-27. OP-20-G (2) (via Lt. Pendergrass)
28. G-2 (via Lt.Col. Hilles)
29-30. S.S.A. (2) (via Major Seaman)
31. Director, S.I.D. ETOUSA (via Lt. Col. Johnson)

TICOM
10. Chairman
11-12. S.A.C. (2)
13. Cdr. Bacon
14. Cdr. Mackenzie
15. Cdr. Tandy
16. Lt.Col. Johnson
17. Lt.Cdr. Manson
18. Major Seaman
19. Lieut. Eachus

Additional
32. Lt.Col. Pritchard

TOP SECRET "U" TICOM/I-19b

REPORT ON INTERROGATION OF

KOMMANDEUR DER NACHR. AUFKL. 1 (KONA..) AT REVIN, FRANCE, JUNE 1945

TICOM
1 July 1945

Copy No. 14
No. of pages: i-v, 1-52.

DISTRIBUTION

British
1. Director.
2. D.D.3.
3. D.D.4.
4. D.D. (N.S.)
5. D.D. (M.W.)
6. D.D. (A.S.)
7. A.D. (C.C.R.)
8. Col. Leatham

U.S.
24-25. OP 20-G (2)
(via Lt. Pendergrass)
26. G-2.
(via Lt. Col. Hilles)
27-28. S.S.A. (2)
(via Major Seaman)
29. Director, S.I.D. ETOUSA.
(via Lt. Col. Johnson)

Ticom.
9. Chairman.
10. S.A.C.
11. Cdr. Bacon.
12. Cdr. MacKenzie.
13. Cdr. Tandy.
14. Lt. Col. Johnson.
15-17. Lt. Col. Pritchard. (3)
18. Major Seaman.
19. Lt. Eachus.
20. Lt. Vance.
21-23. Ticom Files (3)

Corrections to TICOM/I-19b

p i, last paragraph: for "REVIN in the ARDENNES" please read "OBERURSEL". Add, at end of paragraph. "The prisoners were next moved to REVIN in the ARDENNES".

p iii, line 10: for "Army Group North UKRAINE", please read "Army Group Centre (former Army Group, North Ukraine)"

I 196

I N T E R R O G A T I O N
-of-
KDR. d. NACHR. AUFKL. 1.

KONA. 1.

GENERAL.

This unit was engaged in the interception and evaluation of Russian Army, Army Air, and N.K.W.D. signals on the southern half of the front from June 1941 until May 1945. As a result of its work, the Germans were able to obtain an accurate and detailed picture of the Russian Order of Battle on the front covered. They were also able to predict the locality and timing of Russian offensives some considerable time before they developed. These results were achieved more by the close integration of all available sources of information than by the reading of actual cipher messages, though a large proportion of the medium and low grade ciphers used by the Russians were in fact read. The rival claims of T/A and crypt-analysis appear to generate as much heat in the German Army as they do in other national organisations; but an unbiased view of the answers given by the PW's interrogated would probably lead to the conclusion that in the case of the Russian forces the respective value of general evaluation (T/A, card indexes,etc) and pure decodes is about three to one. This is due to two factors :-

(1) The general unreadability of Russian High Grade ciphers, owing to the practically universal use of one time pad.

(2) The enormous amount of information to be obtained from the Russian practice in the use of indicators, call-signs, and the generally low though improving standard of Russian wireless discipline.

From the crypt-analytical angle Russian security is based almost entirely on the use of one time pads for high grade, and a multiplicity of code books and reciphering tables for medium and low grade ciphers. The latter are perfectly straightforward in the systems used and their solution depends almost entirely on the availability of sufficient material. Under wartime conditions the Germans seem, in most cases, to have obtained all they required.

EDITORIAL NOTES.

Some explanation is needed of the form in which the present report appears.

The members of Kommandeur der Nachr. Aufkl. 1 (KONA.1) were first discovered at KONSTANTINSBAD, near PILSEN, at the end of May 1945. There they received their first interrogation. There Ltn. LOEFFLER wrote his first review of Russian ciphers.

Then the unit moved to REVIN, in the ARDENNES, where, at the instigation of the first interrogators, thirty-one further reports were written by the various Ps./W, some by combined effort.

All the available reports were studied before the final interrogators (specialists) proceeded to Revin. Two of the original reports, LOEFFLER's and HEIMANN's (the latter on traffic analysis) were so elaborated during the course of the final interrogation that it is purposeless to record in translation the original versions: they are incorporated in the critical reviews of Annexes 1 and 2 .

The remaining 30 reports appear, below, in literal translation. Well as the prisoners had allocated tasks to the individual reporters, there are many passages which overlap. Classification and arrangement was difficult. Annexe summarises the contents (insofar as they are not already covered in Annexes 1 and 2) of these reports.

Specialists develop their own jargon. Translators were obliged to follow that of KONA 1, e.g. Blocknot, Chi-number, see 'List of abbreviations and equivalents.'

T196

Units and Authorities (not translated)

Gen. d. NA. (General der Nachrichtenaufklaerung) identical with:

LNA. (Leitstelle der Nachrichtenaufklaerung)
Note: Gen. d. NA. is successor title to LNA., the Sigint. organisation of OKH.

KONA. 1 (Kommandeur der Nachrichten-Aufklaerung 1); also referred to by R/W as the 'Regiment'. A KONA. is the Sigint. unit of a German Army Group, in this case, of Army Group North Ukraine.

NAAS. (Nachrichten-Aufklaerungs Auswertestelle): the Evaluation section of a KONA.

Fests 10 (Feste Nachrichten Aufklaerungsstelle 10): an originally static, latterly semi-mobile long range intercept unit: Company strength, with KONA 1.

NAFAK 617, 623 (Nachrichten Fernaufklaerungskompanie 617,623): Long Range Sigint. Companies with KONA 1.

NANAK 954 (Nachrichten Nahaufklaerungskompanie 954): Close Range Sigint. Company with KONA 1.

Abt. 3,4 (Nachrichtenaufklaerungs Abteilung 3,4): staffs responsible for coordinating the Close Range Sigint. effort of Sigint. Regiment and for cooperation with the Armies.
N.B. The writers of the reports use 'Abteilung' of the Abteilungen 3 and 4, and of the subsections cryptoanalysts, evaluators etc. with the various Sigint. units. Please note that in the translations the word 'section' (used to denote the specialist groups) does not imply a sub-unit of any specific size.

FOK. German abbreviation for the Russian 'Frontoberkommando', the HQ. of a Russian Army Group.

Terminology (translated, or semi-translated, or not translated).

additive: Wurm.
code: Code.
key: Schluessel.
recipher: Ueberschluesselung.
stencil: Raster.
substitution: Caesar.
traffic analysis: Funkbetriebsforschung.
traffic evaluation: Verkehrsauswertung.
transposition: Wuerfel.

Blocknot: untransl. -- is One-time pad.
Chi-nummer: Chi-number -- is cipher serial number.
Chiffrant: not transl. -- a recipher element, present in N.K.W.D. traffics only.
Hauptverteiler: given as 'Basic book for Allotment of C/s (Hauptverteiler.)'

(N.K.W.D.) 'Grenztruppen.' Not translated. Apparently the N.K.W.D. troops which operate at the junction-

-- T A B L E of C O N T E N T S --

(N.B. The general headings I, II etc. supplied by editor.)

I 194

IV C R Y P T - A N A L Y S I S, details.

Report No. 24 Aids to crypt-analysis, by Gefr. E. BAHR.
Report No. 25 Crypt-analysis of 5-figure additive code, by Uffz. H. ALTHANS.
Report No. 26 Spring and Fall, change of 5-figure code, by Hptm. R. ROESSLER.

V N. K. W. D. traffics.

Report No. 27 Study of N.K.W.D. traffic, by Ltn. E. WOELLNER.
Report No. 28 Characteristics of N.K.W.D. traffic, by Gefr. L. HUCHTING.
Report No. 29 N.K.W.D. codes, by Obergefr. G. THOMAS.

VI A I R F O R C E traffics.

Report No. 30 Study of Russian Air Force traffics, by Ltn. E. WOELLNER.

Synoptic of original and present report numbers:

1	:	9	11	:	7	21	:	4
2	:	11	12	:	15	22	:	10
3	:	1	13	:	18	23	:	13
4	:	21	14	:	16	24	:	25
5	:	26	15	:	14	25	:	23
6	:	8	16	:	17	26	:	22
7	:	19	17	:	12	27	:	3
8	:	27	18	:	31	28	:	28
9	:	20	19	:	5	29	:	24
10	:	6	20	:	29	30	:	2

I 198

-- R E P O R T No. 1 --

ORGANISATION OF KONA. 1.
(No German title given),
by
Major Ernst HERTZER. (O.C.KONA 1)

A. ORGANISATION.

The Sigint. Regiment (KONA 1) controlled the following forces :-

NAFAK.	617
"	623
Feste	10
NANAK.	954
NAAS.	1

FANAK. 623 was subordinate to Staff, Sigint. Abteilung 3 and FANAK. 617 and NANAK. 954 to Staff, Sigint. Abteilung 4 NAAS. and Feste 10 were directly subordinate to the Regiment C.O.

Up to September 1944 NANAK 953 was also subordinate to Abteilung 3, but it had then to be given up to the West. Only the interpreters and crypt-analysts for Russian remained behind. They were the nucleus of close range sigint forces in the Army area served by Abteilung 3. Specialists of various kinds were withdrawn from each company and attached to Abteilung 3, so that finally a complete close range sigint company was again available to Abteilung 3. This company was named after the C.O., Oberleutnant BENOID.

About the same time it became necessary to establish a close range sigint service in the area of Pz. AOK. 1. (AOK.17 had been pushed up via LEMBERG to the BARANOW bridgehead after the Russian offensive; the (Sigint.) forces previously operating in sector of Pz. AOK. 1 were now operating in the sector of AOK 17, the more important sector.) Again the necessary forces were withdrawn from the other units; the Close Range Sigint Company of Oberleutnant PREUSZ was formed. This company was directly subordinate to the Regiment C.O.

B. DEPLOYMENT.

LONG RANGE SIGINT.

Regiment Staff and NAAS. always operated in the immediate vicinity of the Army Group H.Q. The original plan for the employment of Long Range Sigint Companies was that one should operate with each army staff, at about army level, and cover an army sector. When German withdrawals began, however, this proved impractical; the pressure of work was usually greatest at the very time when the companies had to withdraw. Consequently in the last year, 617, 623 and Feste 10 operated further and further to the rear, in the immediate vicinity of the Staff and the NAAS, i.e. in the vicinity of the Army Group. This ensured more rigid control of interception and evaluation and quicker passing of results.

CLOSE RANGE SIGINT.

The Close Range Sigint. Company always operated by platoons, one platoon with each Corps Staff. Each platoon covered its own Corps sector. The platoon had a strength of 20 to 30 men, about 12 interpreter operators for taking R/T traffic, 2-3 W/T intercept operators for morse, 3 evaluators, 1 Close Range Field D/F section with about 5 men, clerks, drivers, a cook etc.

The platoons reported their results to the Corps Staff and to the Evaluation Section of their Company which was located at Army. The Company Evaluation Section correlated all results from all platoons and reported the combined results (laterally) to Army Staff and back to the NAAS.

C. D / F.

We distinguish between Long-Range and Close-Range Field D/F sets. Long Range D/F sets were employed 200-350 km. behind the front line. 2 to 3 D/F sets in one place constituted a D/F Group; each set would operate for a particular company. Results were reported back by W/T. The most favourable points of intersection and the peculiarity of the terrain were factors taken into account in choosing sites.

The Close Range Field D/F sets were located with the Close Range Sigint. platoons. They served the platoons but also accepted 'Requests' of the Long Range Sigint. Companies. (Which D/F sets received 'Requests' from which Company was arranged in accordance with the situation.) Reports back to the Long Range Sigint companies were made by W/T.

D. COMMUNICATIONS.

In general, the landline net of the Army Group was used; all results could therefore be passed by T/P or telephone. The Army Group telephone construction units made the tappings and undertook major structural modifications. We installed internal lines ourselves. So that work should continue even when lines were down, every unit, whether Abteilung, Company, Platoon, or independent section was equipped with W/T. As soon as a line was down, W/T came into operation. In this case only abridged reports were transmitted.

1194

-- R E P O R T No. 2 --

ORGANISATION OF FESTE 10 .
'Organisation der Festen Nachr. Aufkl. Stelle 10',
by
Obltn. Wilhelm KNAUS (Feste 10).

A. COMPOSITION.

1. Commanding Officer's Group and baggage train.

1 Officer, 20 NCOs and men, 4 female Sigs. assistants and 2 female Staff assistants.

2. Intercept platoon.

30 NCOs and men, 54 female Sigs. assistants.

3. Evaluation.

25 NCOs and men, 8 female Staff assistants.

4. Crypt-analysis.

1 Officer, 15 NCOs and men.

5. Sigs. Platoon.

a) W/T Section, 4 W/T Operators, 3 female Sigs. assistants.

b) T/P: 3 Operators.

c) 'Phone: 3 Operators

6. D/F Platoon.

50 NCOs and men.

B. TASK.

1. Commanding Officer's Group and baggage train:

Supply of Sigs. equipment and vehicles, rations, clothing, kit; also welfare questions.

2. Intercept Platoon.

Cover of:

a) unknown traffics in 3500 - 5500 kcs. band.

b) fixed NKWD nets specified by NAAS.

c) nets of mobile formations as required by NAAS. (some of these nets partly covered also by NAFAK 617 or 623.)

3198

3. EVALUATION:

a) elucidation, interpretation and reporting of new traffics appearing on frequencies above 3500 kcs. Control of cover.

b) exploitation and sorting of intercepted signals. Preparation of 'Advanced Reports'; 'Technical W/T Sitreps'; '5-figure offers' and 'Report on Intercepts.' ø

4. CRYPT-ANALYSIS:

a) translation of P/L signals.

b) solution of new systems and reciphers.

c) contribution to interpretation of unknown traffics by identification of old keys.

5. SIGS. PLATOON.

Responsible for :

a) W/T communication with Rgt. and the D/F sites.

b) passing of all results (T/P or telegram) to NAAS.

c) passing of D/F requests.

6. D/F PLATOON.

Task: to carry out the 'D/F requests' of the Companies.

(The D/F Platoon is not carried on Establishment. It was only possible to set it up with allocated female Sigs. assistants who are carried over and above Establishment .) The platoon comprises :

2	TELEFUNKEN sets,	1 NCO,	5 men
2	RIGA / sets,	1 "	6 "
1	LORENZ (converted)	1 "	5 "
2	LORENZ	1 "	6 "

Plus: 4 M/T drivers.

ø Interrogator's Note: 'Advanced Reports' etc. are titles of specific types of reports. 'Advanced Reports' usually give the text of a single intercept, with comments, or one piece of intelligence derived from traffic analysis. The 'Report on intercepts' is a daily write-up of the day's 'Advanced Reports' plus the residue of intercepts which had not merited formulation as an 'Advanced report'.
'5-figure offers' are described in greater detail elsewhere: They simply list the interpretable elements of the (generally

I194

-- R E P O R T No. 3 --

ORGANISATION AND METHOD OF EVALUATION IN THE COY. AND NAAS.

'Gliederung und Arbeitsweise der Komp. und der Nachrichten-Aufklaerung-Auswerte-Stelle (NAAS).'

by
Ltn. Heinz POGANSKI (NAFAK.623)

A. EVALUATION IN A LONG-RANGE SIGINT. COY.

Consists of traffic evaluation, content evaluation (with card-indexes), D/F evaluation, cryptanalysis, traffic analysis, work on unidentified traffics, N.K.W.D., and fusion.

The working data for these sections are the traffic picture and signals.

Traffic Evaluation prepares network diagrams showing the Traffic relationships in the various networks. The net diagrams include the evidence which has identified the W/T stations; 5-figure characteristics, names which have appeared and further significant characteristics which will enable the traffic to be re-identified. These net-diagrams are the basis of all evaluation processes.

Content-evaluation works on all readable messages, identifies places, names and covernames, solves coordinates and sees to the immediate forwarding of all important messages to the NAAS.

The methods of work of the remaining sections of evaluation are laid down in further reports.

The routing of messages within Coy. Evaluation depends on their type:

a) P/L,
b) 2, 3, 4 -figure,
c) 5 figure,
d) miscellaneous.

All messages go in the first instance to the person responsible for signals headings: he writes the identity of the call-sign against the call-sign. P/L signals then go to the translator, content-evaluation and fusion. 2, 3, and 4 figure messages go through the relevant cryptanalysis section and thence to the translator. Thence, same routing as for clear text messages.

5-figure messages go from the person responsible for headings to the 5-figure index where interpretations are written against the 5-figure characteristics. The traffic evaluator then enters the 5-figure characteristics onto the net-diagram of the traffic in question.

Sigint results are reported to NAAS. as follows :

I194

B. THE ORGANISATION OF EVALUATION IN A NAAS. is as follows :

1) Technical and tactical evaluation of identified traffics (Army traffics picked up by Long Range units)

2) Processing of unidentified traffics (Traffics picked up by Long Range units and Short Range units - the former may contain some which are not Army Traffics).

3) Checking and tactical evaluation of reports from Short Range units.

4) Traffic analysis, D/F evaluation, keeping of card-indexes, N.K.W.D. evaluation, Evaluation of Russian Air Force traffics.

Cryptanalysis in the NAAS. is not, as in the Companies, a section of evaluation, but is an independent section. The NAAS. so organises its work that it may check and carry forward the evaluation work of the Coys., and achieve a synthesis of the various branches of Evaluation and combine the results of Close and Long-Range Sigint; also of N.K.W.D. and Russian Air Force cover. There is more detail on the various branches of evaluation in other reports.

I196

-- R E P O R T No. 4 --

ORGANISATION OF AN INTERCEPT STATION.
'Die Organisation einer Empfangsstelle,'
by
Uffz. Emil HERBST. (NAFAK 623).

1. TASK:

Cover of Russian W/T traffic according to Fronts (1st White Russian, 1st, 2nd, 3rd, 4th Ukrainian Fronts) within the frequencies 1400 - 7000 kcs.

2. DEPLOYMENT (WITHIN A COY.)

Approx. 80 W/T operators were available. Of these, approx. 30 in 2 reliefs, each relief consisting of 15, employed during the day from 0500 to 1700 hours on search intercept, and approx. 50 operators in 3 reliefs (6 hours each), each relief consisting of 17 operators, employed continuously to observe known W/T nets. 1 or 2 receivers per operator.

a) Search intercept. Allocation of a frequency band up to 150 kcs. per receiver (depending on the density of traffic). Recording of all W/T traffic of the Russian Armed Forces including NKWD in the day report, (See day report pro forma), Recognition Characteristics: Q -, Z -, and specifically Russian procedure signals, methods of tuning of wireless station, method of conducting traffic.

When day report had been submitted by evaluation section

1) discarding of traffic of no interest (air force, traffic outside sphere of assignment),

2) intensified observation of traffic passing large volume of messages clearly tactical or strategic.

3) Allocation of traffics belonging to sphere of assignment to receivers for further cover.

b) Receivers on cover. Continuous cover of recognised traffics, according to the degree of importance.

3. D/F SERVICE.

In order to locate transmitters, long contact traffic and signals in known nets were D/F'd, as necessary; also signals in unknown traffic. Control of the D/F stations was exercised by the D/F Request transmitter, which was worked from the intercept station. This was wireless control: we had our own procedure signals to describe the traffics which were to be D/F'd. Every 'Request' had a serial number which was entered in the 'Day Report', and, in the case of signals taken down, also entered on the intercept pro-forma.

I196

-- DAY REPORT PRO - FORMA --

(UNIT) (PLACE, DATE)

Day Report No. ____

from (date,hour) -to- (date, hour)

HOUR	KCS.	TO	FROM	D/F NO.	CONTENTS	MESSAGE NO. 134	
0731	3300	abc	a8y		qrk? nil ok? ec		qsa4
33	"	a8y	abc		ok qsa3 nil sld str ec		" "
				21		134	
45	3315	oki	iwu		ok qsa4 qtc molniae nr 35 gr 50 2io6 o730 (5Z) qsl ? ec		" "
56	"	iwu	oki		ok rdv rdok nr.35 gr. 50 qsl nil ec sk		" "

I 198

-- R E P O R T No. 5 --

ORGANISATION AND TASKS OF CRYPT-ANALYTIC (SECTION) OF NAAS. 1.
'Aufgabe und Organisation der Entzifferung der NAAS 1'
by
Oberwm. Klaus EICKHOFF
(NAAS.1)

The crypt-analytic (section) of NAAS.1 had the following tasks :

1) to collect and work on signals which the Companies could not deal with (whether because of lack of material or preoccupation with more important systems).

2) to test and check doubtful solutions offered by the Companies.

3) to establish whether keys broken by the Companies were the first examples of their kind; to complete them and put them into a handy workable form (the so-called 'basic form').

4) to pass on [M] all solved key systems to Companies who might be interested.

5) to assign a number to each key appearing in the Regiment's area.

6) work on N.K.W.D. signals.

Crypt-analysis in NAAS.1 was, accordingly, subdivided into the following sections [©]:

1) 2-figure
2) 3-figure
3) 4-figure
4) New developments
5) Analysis
6) N.K.W.D.
7) Book building (Code-Ausbau)
8) P/L text scrutiny
9) Organisation.

The sections 1 to 3 looked through the relevant material in both raw and processed state: corrected or made up mistakes or inadequacies in Companies' solutions. (Signals on which no work had been done (at Company level) were, if there was sufficient material, passed to the section dealing with 'New developments'.) They were also responsible for checking the solutions offered in their respective (2,3 and 4-figure) fields.

M Translator's Note: The text has clearly WEITERBIDUNG, which is almost certainly scribal error for WEITERLEITUNG, as translated above.

I196

Section New Developments did the real crypt-analysis. It normally concentrated on difficult systems which Companies had neither time nor man-power to deal with adequately, if at all.

The analytic section consisted, in the main, of mathematicians and its work was of mathematical, systematic or analytic nature :

Work on addresses (2,3 and 4-figure).

" " 5-figure Signals, letter systems (transposition, Stencil).

Examination of Signals with practice traffic characteristics.

Reduction of solved keys to a basic form.

For a time 5-figure signals also were worked on in this section, but this work was soon handed over to Gen. d. NA. ∅

Intercepted N.K.W.D. signals were worked on in the N.K.W.D. section of the NAAS. if they were originated in the Regiment's area. The remainder were sent by courier to LNA.∅

The keys solved by the Companies were passed, as necessary, to the book-building section (Code-Ausbauabteilung), to be completed. This section worked in close contact with the analytic section (task common to both: establishment of basic form of keys).

The section responsible for P/L text scrutiny investigated questionable translations, corruptions, and abbreviations.

The organisation section was in control of all administration, allocation of (German) keys and responsible for reports to Gen. d. NA.

Crypt-analytic sections in NAAS. 1 totalled, according to establishment, 60 men; this strength was never reached, despite increasing difficulties in Russian keys which called for more and more specialists and assistants.

Attached, a survey of Signals intercepted and studied. Figures indicate monthly averages (and correspond to the true figures). ∅

∅ Note: See table of abbreviations; Gen. d. NA. is the successor title of LNA. Ps/W normally said 'LNA' and then added "which is now known as General etc."

∅ Note: Prisoners had no documents. In the majority of the diagrams and tables the figures given are stated to be arbitrary. The 'attached' statistics are on page 44.

-- R E P O R T No. 6 --

ORGANISATION AND TASK OF CRYPT-ANALYTIC SECTION OF A LONG-RANGE SIGINT. COY.

'Organisation und Aufgabe der Entzifferung einer Fernaufklaerungskompanie'

by
Ltn. Harry LOEFFLER
(Feste 10).

Coy. crypt-analysis is organised in the following sections :

1) Clear text translation.
2) 2-figure section.
3) 3-figure section.
4) 4-figure section.
5) General section.

Their duties are apparent from their designation.

The clear text section was responsible for translating, as quickly as possible, incoming clear-text signals.

Sections 2 to 4 had either to decode signals sent in known codes, or to recover new systems.

The general section kept various card indexes and lists, statistics of signals, and had other administrative duties.

An establishment of 15 to 20 personnel was adequate for Coy. crypt-analysis, depending on the type of task assigned. The strength of the various sections was modified to cope with developments on the Russian side: namely, the shifting of emphasis from 2-figure to 3-figure and then later to 4-figure. Special procedures, such as Signal Codes (3-figure and 4-figure), Word Codes and Address Codes (3-figure), were studied in the appropriate section by specially chosen crypt-analysts, for the most part also by the chief crypt-analyst. The average working time to recover a new code varied a good deal, and depended on the difficulties of the procedure. The amount of material required depended on the security of the system. There were systems which were solved in a few minutes with relatively little material. There were others which required a considerable volume of material and a number of weeks' effort before they could be even partially solved.

It was the task of Coy. crypt-analysis not only to solve systems, to recover reciphers, to decode already known procedures and/or to translate all this material, but also to contribute to the identification and interpretation of traffics on the basis of the keys employed.

The latter task was of especial significance in so-called search interception, where all the traffic of a particular area (e.g. on one front) had to be singled out and the remainder dropped. Identification of traffics by key played a role similar to that of identification by call sign usage, frequencies, proper names, covernames etc.

Crypt-analysis cooperated closely with Evaluation and Interception.

Deciphered and translated messages were forwarded to the former (Evaluation) with notes calling attention to the key employed or to other characteristics which would facilitate or confirm an identification. Collaboration between Crypt-analysis and Interception was focussed on :

Special observation of traffics carrying new code systems. This might, in the case of important traffics, lead to better intercept-operators being set to cover such traffics.

Ccy. Crypt-analysis was, strictly speaking, from the point of view of Establishment, part of the Evaluation Platoon. It was, in practice, independent, owing to the special nature of its work. It cooperated closely with Crypt-analysis of the NAAS, but was so organised and equipped that it could work on most messages itself. For the training of crypt-analysts there were short courses of instruction in the training unit. Once trainees had a rudimentary knowledge of the subject they were drafted to field units for further training and practical experience: in certain specialised branches this field training lasted a considerable time.

GENERAL METHOD; Examples of Evaluation.

-- R E P O R T No 7 --

E V A L U A T I O N .

'Auswertung'

by

Hptm. Roman ROESSLER.
(NAAS 1)

Evaluation of enemy W/T traffic (intercepted by Long Range and Close Range Sigint Companies) was carried out according to certain fundamental principles, some of which were evolved in the course of operations; others were hunches of individual workers. There were no prescribed rules for evaluation, and this fact, determined by the material dealt with, made the success or failure of the Sigint Service a personal matter depending on the perspicacity and experience of a few specialists and persons operating in key positions.

A fundamental principle, established after much difference of opinion, was that the smallest detail serving to characterise or identify enemy W/T traffic should be carded; the resultant card index served the most varied purposes. The mass of material intercepted compelled this step; firstly as an aide mémoire, secondly a most careful record of all characteristics became increasingly urgent as, with increasing Russian W/T security, the sources available for interpretation became continually less numerous. Towards the end of the war, therefore, the card indexes were considerably extended, despite economies in personnel and material.

Assessing the efficiency of the various aids to evaluation, we give first place to the card index: It gave direction and continuity to our whole work. This is true in spite of single instances where pure crypt-analysis gave a right answer, e.g. identified an army by means of a decoded signal.

A fundamental principle of evaluation was to take account of <u>everything</u> (regardless of the importance of one phenomenon or the irrelevance of all other similar phenomena.)

Thus the card indexes formed the indispensable <u>material</u> basis for evaluation, memory, experience, and perspicacity of the individual evaluators lent the spark.

In accordance with the above principles Companies had to provide most detailed reports. A smoothly functioning report system was the chief problem discussed at almost all meetings to consider organisation. A Long Range Sigint Company needed an average of 16 typist hours to get out its daily report for the NAAS.

The reporting system covered the following fields (whether in writing, by courier, or by T/P and/or telephone):

1) Report on traffic of the W/T nets (call-signs, frequency, traffic workings, keys used, further characteristics).

2) Report on content of signals.

3) Technical Signals Reports.

The reports of all the Companies, collated by the NAAS., gave a complete picture of the traffic intercepted during the day. The more important conclusions -- those which had tactical value -- deduced from traffic relations and content of messages, were collected in the daily Situation Report (Lagemeldung).

The work of the NAAS. was hardly reflected in these daily Sitreps. (A small group of workers would have been sufficient for current observation and interpretation of known W/T nets.) Since the intercept operator hears a great deal more than just the enemy traffic he has been assigned to, and since by far the greater %age of all intercepted traffic is unidentified, the NAAS. - as also FHQ/TE 10 - had to deal necessarily with all the traffic of the Russian Armed Forces. The interpretation of unknown traffic was, consequently, from a long term intelligence point of view, the chief evaluation problem, and all the elements of the organisation, particularly the card indexes, had to be brought to bear on it.

Comprehensive Research work which served to generalise and/or systematise the detailed evidence was carried on from the same point of view.

Further material which served in identification included:

Names (including those heard in radio broadcasts)
Cover-names.
5-figure characteristics.
D/F results.
(Map) Coordinates.
Key usage.
Contents of decoded signals.
Technical characteristics.

The part played by decoded messages in the total success of Sigint. diminished steadily towards the end of the war. Intelligence of greatest tactical value was drawn mostly from other sources (5-figure characteristics, coordinates).

What is said of the individual branches of evaluation in the following passages can only give a rough and approximate picture. The technique of evaluation in individual instances cannot be systematised.

By and large, Sigint. gave an almost complete picture of the grouping of Russian forces, from the Fronts (Army Groups) via the Armies, down to the Corps.

The strategic mobile formations (Armour and Cavalry) were continuously covered. When formations could not be completely identified (because increasing camouflage measures denied us formerly accessible sources of information) the overall grouping and number of available formations was still clear. Rifle Corps and divisions were usually better known to the IC through other sources (prisoners etc.) In the overall picture, Infantry formations were not as interesting as the Senior HQs, and the mobile formations. It was essential for the IC that Sigint should observe events on the enemy's side which could be learned from no other angle: movements of strategic reserves, building of Schwerpunkts, chain of command, intentions to attack (all seen in broad strategic perspective). With unimportant exceptions, this task was fully accomplished by Sigint.

-- R E P O R T No. 8 --

CARD INDEX SECTION.
'Abteilung Karteien'
by
Insp. Georg BERGER (NAAS.1)

There was a special section in NAAS.1 whose duty it was to look after all card indexes.

NAAS. 1 was the chief evaluation centre within the Regiment: its card indexes had to be as comprehensive as possible. This meant collaboration with other Regiments employed on the East Front (2, 3 and 8) and with G.d.N.A., East. An exchange system (new interpretations, corrections etc.) functioned smoothly by telegraph or courier (depending on urgency).

1) Personality index.
2) Unit index.
3) Blocknot index.
4) Key (SCHLUESSEL) index.
5) Call-sign index.
6) Cover-name index.
7) Coordinates index.

1) This card index contained the names of all officers and W/T operators gleaned from wireless or from IC reports (PW interrogations, captured data, etc.). Example: AIESKOWSKIJ, OBERST. Chief Signals Officer, 1st Ukrainian Front. (Mentioned on wireless on 15/1/'45) or GWANOW, Major. Area 6th Pz.Army (18/2/'45, KONA 8). Names from wireless had to be treated with special caution, since the Russians used cover names for proper names. When such were clarified, a suitable entry was made on the card.

2) This card index contained all units of the Red Army from wireless or from IC. Each card had spaces for the following entries :

a) Unit
b) C.O.
c) Chief of Staff
d) Subordinate to ...
e) Sub-units:
f) Operational locality or area.
g) Date of first appearance.
h) Sources.

3) The Blocknot card index consisted of :

a) Search card index, and
b) Unit card index.

The Search card index contained all known and unknown Blocknots and Chi-numbers which had been picked up.

The Unit card index, on the other hand, contained only known Blocks and Chinumbers, arranged according to unit.

In 5-figure messages the blocknot is one of the first 10 Groups. Its position changed at long intervals, but was always easy to re-identify.

The Russians differentiate between three types of blocks :

1) The 3-block, 'DRIERBLOCK' (also called 'I-BLOCK' = Individual block,) could be used, and read, only between 2 W/T stations in one net.

2) The 6-block, 'SECHSERBLOCK' (also called 'Z-BLOCK' = Circular block,) could be used, and read, between all W/T stations in a net.

3) The 2-block, 'ZWEIERBLOCK' (also called 'OS-BLOCK',) used only in traffic from lower to higher formation.

The Chinumber is the serial numbering of all 5-figure messages passing through the hands of the Cipher Officer, starting on the first of January and ending on thirty-first December of the current year. It always appears as the last group in a message, e.g. 00001 on the 1 January or when the unit is newly set up. The progression of Chinumbers was carefully observed and recorded in the form of a graph. A Russian Corps had about 10 5-figure messages per day, an Army 20-30, and a Front about 60-100. After only a relatively short time the individual curves separated sharply, and the type of formation could be recognized by the height of Chinumber alone.

Distribution of Blocknots. Blocknots are distributed centrally from an office in MOSCOW. Every Blocknot contains 5-figure groups in a number of sheets, for the enciphering of 5-figure signals. It bears a number of 5 digits on the front. Blocknots are distributed as required in packages to the staffs.

Example: The 3rd Gd. Tk. Army transmits a 5-figure message with the Blocknot '37581' (one of the first 10 groups in the message). On the same day the Block '37582' was used by the same formation. The next day '37583' appeared. Thereafter the Army was no longer heard. It was maintaining wireless silence. After a few days an unidentified net with the Blocknot '37588' is picked up. This net is claimed, because of the proximity of the blocks (88/83), to be 3rd Gd. Tk. Army. (The missing Blocknots 84-87 were presumably used in telegraphic telephonic or courier communications). The Chinumber (progression of the curve), provides confirmation of the first assumption (based on proximity of Blocknots) in most cases.

4) The Key card index contained details of all solved 2, 3 and 4-figure procedures whether their provenance (area) was known or not. Every solved key received a number from Crypt-analysis, which thenceforward was the name of the procedure. 2 and 3-figure procedures in particular were peculiar to definite formations, so that on the basis of key alone, conclusions as to the formation could be drawn without risk.

5) The Call-sign card index contained all known and

I19b

6) The Covername card index contained all covernames which had been collected, and indicated, source, and date of occurrence. With the assistance of the card index, we recovered, in many cases, almost complete covername tables for the Russian Fronts.

7) The Coordinates card index contained all solved systems of (map) coordinates of the Russian fronts. It was organised in two parts :

1) Coordinates arranged by systems
2) Coordinates arranged according to units.

NOTE: Russian air traffic was studied in a special section of NAAG. 1.

The system of card indexes above described applies also to the processing of air traffic.

-- R E P O R T No. 9 --

I194

THE ATTACK ON AN UNIDENTIFIED RUSSIAN TRAFFIC BY THE VARIOUS SECTIONS OF EVALUATION

'Arbeitsweise bezw. Zusammenwirken der Abteilungen der Auswertung bei der Erfassung eines unbekannten russischen Verkehrs'

by

Ltn. Hans BOSKAMP (Feste 10).

I) All W/T traffic recognised by its manner of working as Russian was handled in the traffic evaluation section and worked up into network diagrams. The network diagram contained :

1) Net number
2) Date
3) Traffic workings with call-signs.
4) Number and kind of messages, if any, sent.
5) D/F number.
6) BLOCK and CHI-number of any 5-figure messages intercepted.
7) Short P/L texts, if any (including names).

II) Study of the network diagram in the 5-figure section (in case a 5-figure message having been picked up).

1) Identification of the W/T station sending the 5-figure message. (BLOCKNOT used perhaps already indexed as known in the 5-figure card index).

2) Suggestion for identification: a BLOCKNOT with almost the same number in the index.

3) Identification by CHI-number alone (or in conjunction with the BLOCKNOT) checked against the CHI-number graph.

4) Identification of general class (e.g. Army traffic) by other 5-figure characteristics.

III) Study of network diagrams in TA section.

1) General scrutiny of composition of call signs.

2) Determination of area covered by net (Front, Army etc.): comparison of call signs used with 'Basic Book for Allotment of Call-Signs' (Hauptverteiler).

3) Recording and collecting of call signs still unclassified (in order to recover new call sign systems).

IV) Checking of the network diagrams and messages against the card indexes of names, covernames, and cover-numbers.

1) Identification of names and numbers by means of the index; hints for interpretation already entered on the network diagram taken into account.

I194

V) Study of the notwork diagrams in the D/F Evaluation Section.

1) Does the D/F fix, if any, point to an area near the front? If so, probably army traffic ('Front' or 'Army' Area).

2) Does the D/F fix point to the rear area? If so, probably Air Force or L. of C. services.

VI) Final evaluation (Fusion).

1) Decision on the identity of the traffic, taking into consideration :

a) the balance of the results entered on the notwork diagrams by the various sections.

b) results obtained by Crypt-analysis section.

2) Reports to MAAS on :

a) identified traffics.

b) tactical information derived from the messages.

3) Guidance for interception.

a) Cover of less interesting traffic suspended.

b) Special attention to more interesting traffic ordered.

-- R E P O R T No. 10 --

I194

EXAMPLE.

SIGINT. SITREP,
0900/27/4 - 0900/28/4.
'Nachrichtenaufklaerungslagemeldung,
0900/27/4 - 0900/28/4.'
by
Ltn. Oskar SCHWARZ
(NAFAK 617)

FIRST UKRAINIAN FRONT.

In cooperation with formations of the First White Russian Front, 1st Ukr. Front completed the envelopment of Berlin in the area North-east of Brandenburg.

We must reckon with the insertion of a major formation (independent mobile corps or an army), not previously known in this Front, possibly in the area of LIEGINTZ.

1) Confirmed in the area of the Front :

4.	Tk. Army	13.	Army
3.	Gds. Tk. Army	3.	Gds. Army
59.	Army	28.	Army
6.	Army	VII	Gds. Mech. Corps
21.	Army	I	Polish Tk. Corps
52.	Army	I	Gds. Cav. Corps
2.	Polish Army	IV	Gds. Tk. Corps
5.	Gds. Army	XXV	Tk. Corps

2) Tank Armies.

4. Tank Army. Joined up in area NE. of Brandenburg with formations of 1st Ukr. Front attacking from the North, and has thus completed the encirclement of Berlin. Army cooperating with 3 Gds. Tank Army and elements of 13. Army.

V Gds. Mech. Corps. Regrouping out of area Spremberg into area NW. of LUECKENWALDE. Main body of Corps attacking Brandenburg.
For battle reports of subordinate brigades, see Advance Reports.

VI Gds. Mech. Corps. Thrusting via Ketzin into area S. of NAUEN, has joined formations of 1st White Russian Front.

X Gds. Tk. Corps. Unchanged, committed with all brigades in the area of TELTOW. Corps cooperating with elements of VI Gds. Mech. Corps.
For locations of subordinate brigades, see Advance Reports.

93. Independent Tk. Bde. Allotted (temporarily?) to VI Gds. Mech. Corps.

3. Gds. Tk. Army. Unchanged; all formations fighting around Berlin. Schwerpunkt of the Army: E. of TELTOW.

VI Gds. Tk. Corps and VII Gds. Tk. Corps still in the same area (E. TELTOW).

IX Mech. Corps supported by 91. Independent Tk. Bde. in area ZOSSEN-KOENIGSWUSTERHAUSEN. Elements of Corps involved in mopping-up in area of BARUTH.

Army HQ in UENSDORF.

Army Battle HQ in GROSSBEEREN.

For battle reports of subordinate Corps and Bdes. see Advance Reports.

3) Independent Mobile Corps.

VII Gds. Mech. Corps. Still supporting 52. Army in the fighting near BAUTZEN. Corps cooperating with I Polish Tk. Corps. Corps Staff: 10 kms. NW. of BAUTZEN.

I Polish Tk. Corps. West neighbour of VII Gds. Mech. Corps. Corps still with 2 Polish Army. Elements of Corps badly mauled. Corps Staff: 12 kms. NW. of BAUTZEN.

I Gds. Cav. Corps. (W/T) link with 52. Army no longer heard. Corps is presumably now employed on independent task. (Thrust via GROSSENHAIN-RIESA toward S & SE, wheeling SE. toward DRESDEN ?).
Corps Staff: 4 kms. W. of GROSSENHAIN.
Corps HQ.: W. of The ELBE, 6 kms. SE. of RIESA.
Subordinated Div: (7 Gds. Cav. Div. ?) attacking MEISSEN west of ELBE.

IV Gds. Tk. Corps. Unchanged in sector of 5 Gds. Army, attacking, with elements, German formations still in area SPREE-FURTH. Withdrawal of further elements of the Corps which had thrust over the eastern edge toward the west, and employment, likewise in area SPREEFURTH, appears possible.
Corps Staff: Area HOGESWERDA.
Corps BHQ: Transferred from area LAUDA into area SW. of HOGESWERDA.

XXV Tk. Corps. Unchanged in sector of 3 Gds. Army. Elements of Corps continue fighting in area COTTBUS. Corps Staff presumably transferred from area of COTTBUS into area of LUEBBENAU.

4) Rifle Armies.

59 Army. Shifting of boundary with 21 Army toward north, presumably as far as area PRIEBORN possible. Confirmation required.
Offensive intention in area S. NEISSE.
Unidentified Rifle Div. on S. edge of NEISSE receives increased delivery of amn.
Unidentified Arty. Commander (A/Tk. Arty. Regt.) newly appeared in area S. NEISSE.
Gds. Rifle Regt. [illegible]

6 Army. Unchanged. Employed against Fortress BRESLAU.

21 Army. HQ. presumably moved toward W. from area 10 kms. NW. of KAUTH. Otherwise no changes in Army area.

52 Army. Command of operations in area BAUZEN (direction of thrust DRESDEN ?) by Army confirmed. Elements of 52 Army employed there (1-2 Mobile Corps).
(VII Gds. Mech. Corps.
(I Polish Tk. Corps.
(Elements of 2 Polish Army (3-4 Rifle
(Divs.)
German counter attack in area NE. of BAUZEN gained only little ground despite high Russian losses.
Front line 2200 etc: Places ---- ---- ----
Subordinated Corps cooperating closely with elements of VII Gds. Mech. Corps in sector 4 kms. NE. - 3 kms. NW. of BAUZEN.
Corps Staff 4 kms. N. of BAUZEN.

254 Rifle Div. withdrawn from the front; badly mauled.

Gds. Mortar Rgt. 'LIMA': Subordinated Abt., previously allocated to 254 Rifle Div., will support, after withdrawal from Div., a new, as yet unidentified, Rifle Div.

5 Guards Army. Unchanged, supported by IV Gds. Tk. Corps. Elements of Army cooperating with unidentified Bde. of the Corps have thrust via RUHLAND toward the West. Further elements of the Army also fighting German formations in area Spreefurth.
HQ. unchanged, in area SE. of Spremberg, continues to bring forward 3 subordinated Rifle Corps.

13 Army. Supporting, with elements, attack of 4 Tk. Army. Army with presumably only one Corps in area S.E. of Brandenburg in the front is regrouping both remaining Corps from area FENSTZRWALDE - LUCKAU in WNW. direction, possibly in area WITTENBERG - TREUENBRIETZEN.

28 Army. The large formation brought up out of area LIEGINTZ via COTTBUS into area S. of BERLIN (cf. Sigint. Sitrep 19/4), is 28 Army. Collaboration with 3 Gds. Tk. Army possible.

3 Gds. Army. Supported by XXV Tk. Corps, unchanged. Army fighting with all formations committed against elements of German 9 Army, who are fighting their way back toward the west.
Schwerpunkt of fighting MARK. BUCHHOLZ.
HQ transferred from area 12 kms. S. of COTTBUS into vicinity of LUEBBEN. Subordinate formations still XXI, LXXVI, and CXX Rifle Corps.

-- R E P O R T No. 11 --

INTRODUCTION OF A NEW FRONT AND ITS EFFECT ON N.K.W.D., AIR, AND ARMY TRAFFICS .

'Das Einschieben einer neuen Front und die Auswirkungen auf den N.K.W.D.-,LW-, und Heeresfunkverkehr'

by
Ltn. Eduard WOELLNER
(NAAS.)

1) N. K. W. D.

a) A new W/T station is heard in the net of the Fronts and the Central Authority in MOSKOW. According to the W/T station number, it must be the station of the Chief of the N.K.W.D. with a Front Head-Quarters. The grouping of the new Front is apparent from the W/T picture (lateral workings), the location of the Head-quarters can be fixed by D/F.

b) One or more nets appear. Call sign usage indicates a Chief of N.K.W.D. troops (attached to Front Head-quarters) with subordinate Regiments. By D/F, location of the Headquarters and approximate extent of the Front (D/F of the Regiments) can be established. By D/F, and interpretation of indicators, and CHI-numbers the affiliation of stations under (a) and (b) and of nets forward of the Regiments can be established.

2) AIR FORCE.

a) Air Force nets appear; judging by the rise in CHI-numbers, an Air Army must be present. As previously unknown BLOCKS and new names appear, it must be a new Air Army. Since in general each Front has only one Air Army (only exception; 1st White Russian Front), it is probable that a new Front has appeared.

b) Message content and D/F of ground units and flying formations indicate a gap between two Air Armies which had previously been adjacent.

3) ARMY.

a) New Front HQ. nets appear and are identified by 5-figure and call-sign usage.

b) Sigint shows gaps between the old, previously adjacent, Fronts.

c) The Armies on the wings of both formerly adjacent Fronts drop out of the HQ. nets.

d) The new Front is mentioned in supply traffic, address of a 5-figure message, or in W/T of forward units.

It is unlikely that all the above pointers will in fact appear. But two of them would be sufficient to

I19b

-- R E P O R T No. 12 --

EXAMPLE.

APPEARANCE OF A NEW MAJOR FORMATION IN
1st UKRAINIAN FRONT.
'Beispiel: Auftreten eines neuen Grossverbandes im
Bereich der 1. ukr. Front.'
by
Lt. Oskar SCHWARZ (NAAS.)

I. REPORT:

a) Sigint sitrep 9/4 ... another heretofore unidentified HQ. (Army, Independent Mobile Corps ?) picked up.

b) Technical argument :

1) Unidentified HQ: besides the well established command channels of the Front (HQ. to the Armies and independent Mobile Corps:) a new channel from the Front has cropped up. Recognised by:

Method of conducting traffic,
Use of frequencies (Traffic Evaluation)
Use of call-signs (T.A.).

2) (Army or Independent Mobile Corps ?) :
Previous experience shows that characteristics noted in (1) occur only in command channels to Armies and Independent Mobile Corps. (Question mark shows we are uncertain which of the two solutions is correct).

II. REPORT.

a) Sigint Sitrep 10/4. The HQ. reported in Sigint Sitrep 9/4 is an Independent Mobile Corps, possibly V Guards Mechanized Corps (previously in 4th Ukrainian Front area).

b) Technical argument:

1) Independent Mobile Corps: Height of CHI-number (5-figure evaluation).

2) Possibly V Guards Mechanized Corps: height of CHI-number (5-figure), name of Russian W/T operator (proper names), W/T channel from HQ. 4th. Ukr. Front to V Guards Mechanized Corps has disappeared. (Traffic Evaluation).

III. REPORT.

a) Sigint Sitrep 11/4. V Guards Mechanized Corps confirmed in 1st Ukr. Front Area. Possible that it is operating in 59th Army area. Tentative identification of 10/4 confirmed.

b) Technical argument:

1) Height of CHI-number, proximity of BLOCK (5-figure evaluation).

2) W/T operator's name confirmed (proper-name index.)

3) 3-figure address.
Possible that it is operating in 59th Army Area:

1) Operational message (5-figure) of 59th Army via Front HQ. to V Guards Mechanized Corps. (Traffic Evaluation).

2) Uncertain D/F fix on Corps Staff in 59th Army Area. (D/F evaluation).

IV. REPORT:

a) Sigint Sitrep 13/4. Bringing up of V Guards Mechanized Corps into 59th Army Area, (1st Ukr. Front) confirmed. We expect it to operate on right wing of Army.

b) Technical argument:

1) Bringing up confirmed: V Guards Mechanized Corps appears in Army command net of 59th Army. (Traffic Evaluation.)

2) Operating on right wing: Corps staff moved forward out of rear Army area to the right wing of the Front, and is in forward area (D/F Evaluation).

I 196

-- R E P O R T No. 13 --

SHIFTING OF SCHWERPUNKT; THE NORTHERN WING OF A FRONT INTENDS TO ATTACK.
'Schwerpunktverlagerung u. Angriffsabsichten am Nordfluegel einer Front ',
by
Lt. Heinz POGANSKI (NAFAK 623).

The situation is: a Front, consisting of 1 Tank Army, 2 mobile formations and 5 Infantry Armies has been on the defensive for 4 weeks. Wireless traffic (strategic) is restricted to contact Traffic and chat.

The following phenomena indicate a shifting of Schwerpunkt and intention to attack.

1) A new W/T station appears in strategic wireless traffic on the northern wing of the Front (D/F) and begins to work with the Army on the Northern wing and the Front's Tank Army (hitherto located on the Front's Southern wing). It could be either a Battle HQ. of the Front itself or a newly brought up formation (mobile or infantry?).

2) The Tank Army reports on 5/6 'am moving'.

3) An Echelon of the Front HQ. appears; according to uncertain D/F bearings it is moving north.

4) The mobile Corps of the Front (hitherto on Southern Wing) tries to contact the Infantry Army on the N. wing.

5) A Guards Mortar formation has, according to Close Range Sigint. received 4·5 consumption units of fuel.

-- R E P O R T No. 14 --

SHIFTING OF THE BOUNDARY BETWEEN 1st AND 2nd ARMY. SIMULTANEOUSLY THE CORPS ON THE RIGHT WING OF 1st ARMY PASSES TO 2nd ARMY. X

'Verlegung der Trennungslinie zwischen '1' Armee und '2' Armee bei gleichzeitigem Unterstellungswechsel des rechten Fluegelkorps der '1' Armee unter '2' Armee.'

by
Lt. Klaus WEIHE (NAAS.)

The following recognised by means of :

first Close Range Sigint. (Evaluation of signals content).

second' Long Range Sigint (Traffic Evaluation and D/F).

1) Move of boundary; simultaneously, formations of '1' Army taken over by '2' Army.

   a) A signal shows GHQ. troops (Guards Mortar units) on the left wing of '2' Army are moving into the sector hitherto held by '1' Army.

   b) Reference in traffic of forward formations on the right wing of '1' Army to the 'new high-ups' (neuer grosser vorgesetzter).

2) Right wing Corps of '1' Army passes to '2' Army.

   a) A new W/T station in the Command net of '2' Army.

   b) W/T station has characteristics of previous right-wing Corps of '1' Army (5-figure characteristics, Chi-number)).

   c) W/T station is D/F'd in known location of previous right wing Corps of '1' Army .

X Translator's Note: Inverted commas indicate these numbers are arbitrary.

I 198

-- R E P O R T No. 15 --

CONTRIBUTION (IN TERMS OF A PERCENTAGE)
OF VARIOUS MEANS OF IDENTIFYING
(W/T STATIONS)+

"Anteil der Deutungsquellen,"
by Hptm. Roman ROESSLER (O.C. NAAS.)

5-figure interpretation,

as sole source: 65 - 70%
in conjunction with 4-figure: 90%

Decodes: 5 - 10%

P/L: 1 - 2%

Cover-names: 15%

Proper-names: 5%

Procedure signals and traffic picture: 1%

Call-sign usage as sole source: 8%

" in conjunction with recurring call-signs & frequencies : 10%

+ Note: "W/T Stations" supplied by Interrogator/Translator. The statistics apply strictly to this one process.

I 196

-- R E P O R T No. 16 --

From personalities & cover-name index "Namen", by (combined effort)

JEREMENKO	C. in C. 4th Ukrainian Front.
MOSALENKO	GOC. 38th Army.
KRAWTSCHENKO	" 6th Gds. Tank Army.
KATUKOW	" 1st Gds. Tank Army.
POLJUBOJAR	i.C. IV Gds. Tank Corps.
KORTSCHAGIN	i.C. VII Gds. Mech. Corps
SCHRAGIN, ALESKOWSKY, PJANOW	Sigs. personnel with H.Q. 1st Ukr. Front.
SCHACHRAJ	Head of Cipher office of HQ. 1st Ukr. Front.
ANISSIMOW	Chief QM. " " " " "
SOKOLOW	C. of S. " " " " "
UMFORMER	Cover-name of 59th Army.
GUSJEW	C. in C. 21st Army.
PUCHOW	" 13th Army.
GORDOW	" 3rd Gds. Army
FILM	Cover-name of 1st Ukr. Front.

-- R E P O R T No. 17 --

(From Unit card index)

(No German title)

by: ? (combined effort).

Notes: "F" means wireless psendonym. Ic means: information from German IC

4 Tank Army

4 Tank Army	VI Gds.Mech.Corps.	V Gds.Mech.Corps.	X Gds. Tk. Corps.
Cover-names			
ROSCHTSCHA			
SAHLYK	LIWER		PYRAMIDER
C.inC.			
LELJUSCHENKO	WORNOW "F"	DAWIDOW "F"	GEOMOW "F"
OGNEW-DONSKOJ "F"			AKULOW,Ic,"F"
BZYRIN "F"	JAWORSKIJ,Ic,"F"		
OSTROWSKIJ,Ic,"F".			
	(etc)		(etcetera)
i.C. Brigades			
OZEROW "F"			
MORELW "F"			
Chi-Number on 1/5:			
about 1500	about 600	about 650	about 500

3rd Guards Tank Army.

3 Gds.Tk.Army.	VI Gds.Tk.Corps.	VII Gds.Tk.Corps.	IX Mech. Corps.	91 Indep. Tk.Corp
C.in C.				
RYBALKO, Col. Gen.				
LIWCHIZ, CSO,"F"		etcetera		
BOUSOW, Col., SO.				
(etc)				
Chi-Number on 1/5:				

-- REPORT No. 18 --

TRAFFIC EVALUATION, IDENTIFICATION OF TRAFFICS

"Verkehrsauswertung, Erkennen der Verkehre",
by Obergefr. Gerhard SCHOLZ.

I. Front HQ. (FOK) Command nets.

Line traffic on two frequencies with periodically changing call-signs.

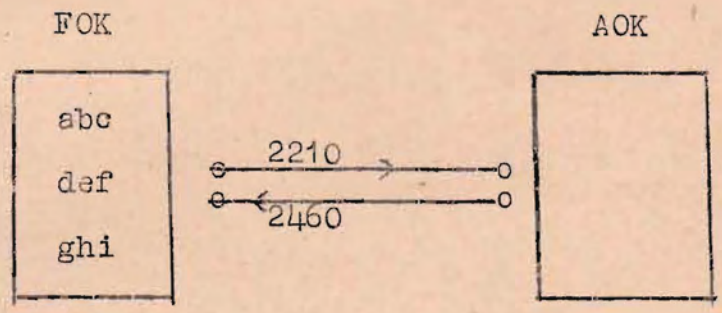
Every formation directly subordinate to FOK (Army, Corps) has two lines.

These can be identified by

1) Frequencies (unchanging frequencies, about 2210, 2400 kcs.)

2) Signals transmitted
   (a) 5-figure characteristics (Blocknot, Chi-number, cover-names, proper-names)
   (b) Cipher signals (key usage, addresses)
   (c) Contents of signals (P/L and decoded signals)

3) Call-sign usage (call-signs taken from a definite table, (perhaps) every third line)



II. Army Command Nets.

Army links with all subordinate formations comprise one or two nets; there is further a net for each 2 or 3 formations. In all, about 6 to 8 nets. Frequencies in 1800 - 4500 kcs. band, but mainly in 2600 to 3400 kcs. band. Each net may have about 3 frequencies (main or working frequency, alternative or spare frequency, calling frequency).

Identification by:

1) Working (star, Kreis & Netz)

2) Signals transmitted (see under FOK Nets, 2a,2b,2c)

3) Call-sign usage (see " " " 3).

III. Corps Command Nets.

Reidentification of a Major Armoured Formation withdrawn from Front.

"Wiedererkennen eines aus Front herausgezogenen Panzergrossverbandes"

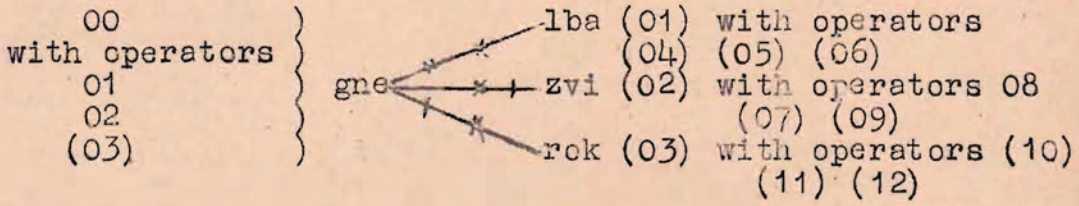
by Inspr. Georg. BERGER (NAAS)

When the Russian Spring offensive of 1944 stopped at the VISTULA, W/T silence descended on the operational nets in the area of 1st Ukrainian Front. A few lines of the Front HQ. were occasionally heard testing. Naturally, the main effort of Evaluation thenceforward lay in the study of unidentified traffic.

Several nets stood out from the mass of unidentified traffic. Special characteristics in their manner of conducting traffic, the structure and transmission of their messages, led to the following interpretation:

Net No.1.

3050 kcs. 1/9/1944



The bracketed Nos. supplied; later confirmed.

Transmission of messages:

Time of intercept

0690/lba/gne - No.6,Gr. 50:

00001	00109	06000
45678	98765	03456
56879	32109	etc.

0720/lba/gne - No.7, Gr. 52:

00001	00109	07100
12345	62890	etc.

1530/rok/gne - No. 10, Gr. 50:

00002	00109	15100

(groups as above, (series of figures).

1600/gne/zvi - No.3, Gr. 57:

00208 00109 15450 etc.

First investigation of above messages revealed:

1) First group - indicator? as yet unexplained

4) Regular sequences of figures point to practice messages.

Further evidence of this: messages of about equal length, 5-figure indicators (BLOCKNOT, key indicator, and CHI-number) usual in operational traffic, lacking.

After this much had been established, the net was reported as particularly interesting to a Company and D/F task allotted.

On 2/9/44, picture was as follows:

Net No.1

3050 kcs. 2/9/44

03 with operator 10.

Time of Intercept.

0130/zvi/gne - No.13, Gr. 53:

00001 00209 00400 etc.

0410/zvi/gne - No.14, Gr. 51:

00001 00209 03500 etc.

0500/gne/rok - No.1, Gr. 58:

00310 00209 04350 etc.

0810/lba/gne - No.17, Gr.50:

00002 00209 07500 etc.

D/F fixes gave points of intersection and triangles of error for all stations in the general area of LWOW. While the control station (recognised as such from the intercept picture) could be located in LWOW, the fixes of the out-stations were different every day. It was assumed that the out-stations were mobile and changed their locations whilst engaged in a W/T exercise. This assumption was confirmed by P/L messages saying: "We are moving" or "We are closing down for a change of location", etc. Further a few operators names turned up in chat.

Further investigation of the message beginnings confirmed the interpretation of the 2nd and 3 groups as date tactical time group respectively.

The 1st group was interpreted as follows:-

00001 =
1st element = dummy.
2nd and 3rd elements = number of W/T Station.
4th and 5th elements = number of operator at keyboard.

This signals exercise lasted from 1/ to 10/9/44. 8 nets were picked up in the course of the exercise. Their stations, and operators, were numbered serially. As a result

The contents of the P/L messages sent made it clear that the nets represented the set-up in the signals exercises of a major motorised formation. A further clue to this was the number of nets (8).

Somewhat later, about 15/ - 20/9/44, a net with operators' names from the above mentioned practice traffic was picked up and D/F'd in the rear area of the 1st Ukrainian Front. According to P/L and 3- and 4-figure messages of the Front M/T Authority, the formation was receiving continuous replacements of ammunition and fuel. Further, bringing up of stocks of tanks was announced. As observation proceed, it became apparent from proper-names and 5-figure indicators (BLOCK and CHI), that the formation was the 3rd Guards Tank Army.

-- R E P O R T No. 20 --

The Study of unidentified traffics

"Bearbeitung unbekannter Verkehre"
by Uffz. Ruprecht STROHTMANN. (Feste 10)

Purpose: To elucidate traffics intercepted on search, which, though recognised as Russian, were not yet identified..

To establish whether they were Army, Air, N.K.W.D. or Partisan traffics. Within our special field the main task was to discover new Army traffics, or to reidentify known traffics using changed signals data.

Means: A whole Sigint Company (Feste 10) was available in the area of KONA 1 for the task of discovering & elucidating unidentified traffics.

Work on unidentified Russian traffics. Traffic Characteristics as a means to identification (Deutungsquellen).

A: Means of rough identification (whether Army, Air, N.K.W.D. or partisan traffic).

1) Call-sign usage (See Traffic Analysis)
N.K.W.D: only means of establishing the Central N.K.W.D. authority is call-sign usage (W/T Station numbers).

Army and Air: from call-sign usage it is possible, provided the call-signs are taken from the "Basic Book for Allotment of Call-signs"(Hauptverteiler), to say whether in all probability the user belongs to certain Fronts, or not.

Aids to call-sign study:

(a) The "Basic book for allotment of call-signs"
(b) Call-sign card-index: contains all call-signs which have appeared, with a reference (by Network No.) to records of the traffic involved. This index helps in re-recognition of previously known traffics (say, in instances where call-signs work according to cycles); it serves also to build up new call-sign squares or call-sign Blocks.

2) Manner of working, procedure signals.

Manner of working and procedure Signals used permit identification, with a certain degree of reliability, of Air, Army traffics etc.

Partisan W/T: can be identified with certainty: they use one call-sign only; most signals are transmitted blind; they use the international abbreviations of amateur wireless, e.g. CK for number of groups; Their 5-figure signals have neither Block nor Chi-number.

N.K.W.D: The procedure group QCO together in the preamble with NK indicates, with high degree of

Air: preference for qco (instead of qtc): wzd (air raid warning signals); met. signals.

Army: Absence of the above characteristics. Latterly on the 1st Ukrainian Front, line traffic using 2 frequencies and 3 call-signs for the line.

3) Types of Signal, Signals content, cryptographic characteristics.

Partisan: 5-figure signals only; No Block or Chi-No.

N.K.W.D: 4 and 5-figure signals with indicators, also some isolated 3 and 2-figure signals (operators' technical chat).

Air: More P/L than in Army traffics; 2 to 5-figure signals; met. signals with unmistakable characteristics (Groups with XXX) - Air Recce reports mainly in P/L. etc.

Army: Practically no operational signals in P/L (Exception: reports on "enemy", including reports on reconnaissance of (against) "enemy"). 3 to 5-figure signals, 4 letter (Stencil)+, 5 letter (machine) + signals (of MOSCOW General Staff). 3 and 4-figure encoded signals often contained P/L groups.

+ Interrogator's note: interpolation supplied verbally by P/W.

B. Means of final identification of a previously unidentified traffic:

1) Contents of decodes (units are practically never mentioned by name in P/L signals of Corps, Armies and higher formations).

Card index of keys: identification by means of key used is possible as, generally, one code is used only by one unit.

2) 5-figure signals: the most reliable and by far the most important means of identification.

On Blocknots, their distribution, Chi-number, 5-figure card index, Chi-number graphs, see 5-figure index.

3) Further means of identification: Cover-names (including officers' psendonyms) in P/L signals, Proper-names in uncamouflaged form in encoded (rarer in P/L) signals.
Details in paper on Card Indexes.

D/F bearings are most important. Location of a W/T Station by D/F makes it possible to exclude immediately, say all L. of C. authorities and formations not conducting operational traffic. The location of a W/T station by D/F in conjunction with evidence of types discussed above inevitably permits clear identification.

I 196

- - R E P O R T No. 21 --

D/F EVALUATION

"Peilauswertung",
by Lt. Edward WOELLNER (NAAS).

Russian wireless discipline and cipher security became better and better: D/F became consequently one of the most important branches of Sigint. Improvements in our equipment and improved (wireless) "Request" systems enabled us to fix a W/T station,

by long range D/F within 15 kms.

" close " Field d/F" 2 to 3 kms.

NAFAK 617 (covering 1st Ukrainian Front) sent its requests, for example, to 3 to 4 long range and about 12 close range D/F sites. The D/F units reported back in enciphered wireless signals to Company. The reports were deciphered and given preliminary evaluation at Company - obvious losers were eliminated. All usable results were reported (bearing and class of bearing) to NAAS which gave its final judgment on, and interpreted, the bearing.

A card index, recording the various bearings on each W/T Station, helped NAAS to judge the value and significance of each bearing.

-- R E P O R T No. 22 --

Re-identification of Individual W/T Stations

"Das Wiedererkennen von einzelnen Funkstellen",
by Uffz Arno GRAUL (NAAST)

Knowing how important it is to be able to re-identify individual W/T stations, I started about 3 months ago to construct an apparatus which would permit re-identification of individual W/T stations by their characteristics. ..

The method: to register the incoming telegraphic traffic in the form of an image on a cathode ray tube (BROWN'SCHE ROEHRE) and analyse the image. Analysis consists of a number of steps, so that all details and peculiarities of the transmitter are comprised. The apparatus is attached to a normal intercept set. The individual characteristics of the transmitter can be recorded graphically by means of tracings, or in the form of photostats, in a card index.

-- R E P O R T No. 23 --

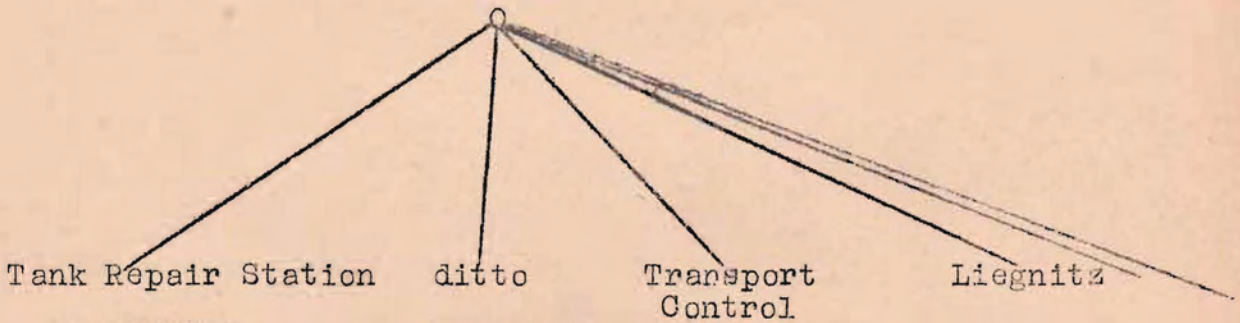
(Network diagram of)
Tank administration of 1st Ukrainian Front.

"Panzerverwaltung 1 Ukr. Front"
by: ?

3960 kcs; 4070 kcs; 3480 kcs (3230)

3 call-sign periods

OZM; ? ; ? ;



Names.

KOGEL, TARASENKO, KUPER } at Control

LEWINSON, MILJAWSKI, ORLOWSKIJ } at outstations

BORISOW, ANANIKAW } mentioned.

Aids to Cryptanalysis
"Die Behelfsmittel der Entzifferung"
by Gefr. Eberhard BAHR (NAFAK 617).

The aids to cryptanalysis, , in the order in which they are used in breaking a message, are as follows:

1) The call-sign index: a card index in which the call-signs were entered of processed messages together with the key used and the date of use. This card index was naturally only useful where there was no daily change of call-sign; i.e. particularly the case of the Russian Air Force.

2) Card index of keys. An index of keys arranged numerically (German numbers) with date and area of use. Purpose. Identification of unknown traffic by known key.

3) Card index of units. Formations arranged according to their numbers, together with the keys they had used.

4) List of indicators and "shift groups". A numerically arranged list of the key indicators used in known keys - they were placed at the beginning and often at the end of messages - - and of the shift groups, ("read letters," "read words") with information on key.

5) Graphic and statistical presentations of letter frequencies,

(a) Average frequency of Russian letters based on military texts of about 10,000 letters. (Order: o, e, i, a, n, u...)

(b) Same for bigrams and trigrams (= 2 or 3 successive letters, reckoned as so many to the thousand): e.g.

AEM	12,2 o/oo	
AEN	10,8 o/oo	
AEP	1,6 o/oo	
AER	10,8 o/oo	
AES	0,4 o/oo	
AET	18,1 o/oo	etc.

6) Intervals. A collection of words where a repetition of letters gives a characteristic picture. Example: NEMEDLENNO, "immediate" shows the following interval:

```
N E M E D L E N N O
x o   o     o x x
1 2 - 2 - - 2 1 1
```

The collections contains not only words, but frequently recurring phrases, which can lead to a break, e.g.

```
  1       2       2 1     2
p O tsch E m u n E O t w E tsch a e sch j  (= Why
```

7) Keys. The keys were entered on the following proformas and divided according to whether they were 2,3, or 4-figure:

	0	1	2	3	4	5	6	7	8	9	
0											0
1											1
2											2
3											3
4											4
5											5
6											6
7											7
8											8
9											9
	0	1	2	3	4	5	6	7	8	9	

Following also noted on pro-forma: date, call-sign, frequency, and, in case known, area:where used.

8) Captured documents. These were of little value for practical purposes. They were occasionally interesting because they gave a general picture of a basic code, which was important, particularly in the case of semi-hatted, and hatted codes.

Following also belong in a cryptanalytic section: dictionaries (general and signals dictionaries), list of Russian military abbreviations, complete list of Russian formations and units, a morse code to check mistakes in interception.

-- R E P O R T No. 25 --

Cryptanalysis of 5-figure additive code
"Entzifferung des ueberwurmten 5Z - Codes"
by Uffz HEINZ ALTHANS (NAAST).

Succesful Cryptanalysis is possible only if

1) there are a number of messages, at least three, which have had the same additive applied.

2) the 5-figure code was captured.

Cryptanalysis starts from the mathematical rule that the difference between 2 code groups remains constant if both have had the same additive row applied to them.

For example.

	Code group	Additive	Cipher group
	39214	20186	59390
	98315	20186	18491
Difference	41909		41909

The most important cryptanalytic aid was therefore the catalogue of differences, a numerically arranged table of the differences between the most frequently used code groups.

Directly the code (which changed approx. semiannually) was captured, about 1000 frequently used clear groups (Positionen) were written out by Gen. d. N.A., arranged and serially numbered according to frequency, and then each subtracted from the other, non-carrying, by Hollerith machines, and entries made on the catalogue as follows:

"41909 17 - 32"

which means:	Nr. 17	u	39214
	" 32	TUPE	98315
	Difference		41909

In the year 1943 KONA 1 for a period did 5-figure cryptanalysis independently (of Gen d. N.A.). For this purpose a difference catalogue of 200 clear groups (= 19900 differences) was compiled by hand.

Calculation aid: A wooden frame with 5 paper belted wheels, I to V, - (1 wheel for each digit of the 5-figure group). Marking of the wheels.

(+ The 0 column contains in each instance the first digit of the 50 selected rods

	I									
	+									
	0	1	2	3	4	5	6	7	8	9
1)	6	7	8	9	0	1	2	3	4	5
2)	3	4	5	6	7	8	9	0	1	2
3)	9	0	1	2	3	4	5	6	7	8
4)	7	8	9	0	1	2	3	4	5	6

On wheel II in each instance the 2nd digit of the code group stood in the 0 column, etc.

Use of the apparatus:

The reciprocal value of a code group is set up above the line by turning the wheels, e.g. 47396 corresponds to 63714 = C. The 50 differences between the latter C and the 50 selected clear groups will then be automatically underneath.

	I	II	III	IV	V
C	4	7	3	9	6
1	6	2	1	5	8
2	7	5	9	3	8
3	4	9	Ø	1	7
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

For example,
62158 = C - 1 Entry in the catalogue 48952 1-C
49017 = C - 3 " " " 49017 C-3

The apparatus also serves as an aid in actual decoding, when a great deal of non-carrying addition or subtraction must be done.

Survey of Successes in Cryptanalysis

Type of Message	Intercepted	Dealt with	o/o	Remarks
2-figure	140	125	90	
3-figure	6,000	2,600	43	
4-figure	5,000	1,900	38	
Mixed	2,350	865	37	
Total	13,500	5,500	41	= Degree of crypt-analtic success.
Clear Text	6,000	6,000	100	
Practice	500	500	100	
Grand total intercepted less				
5-figure & N.K.W.D.	20,000	12,000	60	
5-figure	8,000	-	-	Not studied at KONA 1
N.K.W.D.	2,000	-	-	Only partially studied at KONA 1.
Grand Total	30,000			

Figures are estimated monthly average for year 1944.

-- R E P O R T No. 26 --

SPRING AND FALL; CHANGE OF 5-FIGURE CODE,

"Fruehlung und Herbst; Wechsel des 5Z-Codes",
by Hptm. Roman RÖSSLER.

C/S Systems:

4-letter - April 42

3-letter - April 43

RBT - June 44

RT44 - July 44-

February 43. PT 42 replaced by PT 43 (only for procedure messages, no more spelling). Appearance of addresses; replacement of indicators (5-figure).

June 43. Appearance of Signal Codes.

January 45. Cryptanalysis: Intensified multiple and serial+ encipherment.

+ Translator/Interrogator's note: MEHRFACH und BANDBEZIFFERUNG. Verbally explained as follows.

If a code is so arranged that many different figures (say 1,3,8,9) can indicate a line or column, the Germans say it is mehrfach-beziffert.

If the same can be indicated by "17-24" or "27 - 32" (i.e. by any number between 17 and 24, 27 and 32) it is band-beziffert.

V. N.K.W.D. T R A F F I C S.

-- R E P O R T No. 27 --

Study of N.K.W.D. Traffic.

"Bearbeitung von NKWD-Verkehren",
by Lt. Edward WOELLNER.

N.K.W.D. traffic was always covered: but only by Long Range Sigint. Evaluation and Cryptanalysis were done by NAAS.

When W/T traffic was restricted during W/T silences, N.K.W.D. traffic was often the most important source for Sigint. At such times, it was more completely covered. When Army W/T was in full swing, coverage of N.K.W.D. was correspondingly reduced. On an average 6 - 12 receivers were employed exclusively on N.K.W.D. cover.

In general the following nets were covered:

1) Chief (N.K.W.D.) authority in MOSCOW with (N.K.W.D. at) the Front HQs.
Reason: The (N.K.W.D.) W/T picture, gave indications of groupings, or the insertion of new Fronts. For example, appearance of a new W/T station communicating with 1st and 2nd Ukrainian Fronts showed that the 4th Ukrainian Front had been inserted between the 1st and 2nd Ukrainian Fronts. In addition the (new) Front HQ. could be fixed by D/F.

2) Front staffs with the "Grenztruppen" Regiments.

Reason: D/F of the Regiments revealed the approximate extent of the Front; D/F of the Chief of Security Troops with the Front High Command indicated the location of the Front HQ. Besides, when a (forward) echelon of the Chief of Security Troops with the Front HQ appeared, it was possible to deduce that the Front HQ would move. This, on the basis of N.K.W.D. traffic alone.

3) Regiments to Battalions.

Reason: Most of the messages could be read; they mentioned Army units by name. e.g.,

(a) Before the attack from the NEISSE sector (1st Ukrainian Front), a 2nd Army and 3rd and 4th Field Replacement Rifle Regiment were mentioned by III Bn. of the 83rd "Grenztruppen" Regiment (operating in GOERLITZ area).
Conclusion: 2nd Polish Army newly brought up to the NEISSE sector.

(b) Lines of advance and boundaries of battalions were mentioned. Battalion boundaries often proved to be Army boundaries.

Traffic of rear N.K.W.D. troops and of the Signals Regiments were of no interest, and were not covered by KONA 1.
For technical details of N.K.W.D. traffic and its characteristics, see "N.K.W.D."

-- R E P O R T No. 28 --

Characteristics of N.K.W.D. Traffic
by Gefr. Leonhard HUCHTING (Feste 10).

The traffic of the N.K.W.D. formed a special group of Russian wireless traffic. The distinction applied equally to the manner of conducting trafficand to the messages themselves.

Four-figure and five-figure N.K.W.D. messages could be easily distinguished by their characteristics from Army and Air Force messages. The first group is a discriminent which in most cases remains constant for one line of traffic. The penultimate group contains the date and a number representing the number of groups in the message less a variable number according to the number of indicator groups used. The last group is the Chi-number (see 5-figure Card Index). Exceptions to these rules are very rare. Two and three-figure messages usually contained technical'wireless chat'.

Operators could usually distinguish N.K.W.D. traffic from other Russian types of traffic.

The letters NK are given in the preamble, but tuning is not carried out by keying "V" as is the practice with international and other Russian traffic but by a simple series of dots and dashes.

The wireless networks could be divided into two main groups

1) Networks of the Central Authority

2) Networks of Formations.

1) The Central Authority's Networks can be further subdivided into:

(a) Central Authority of the Security troops.

(b) Central Authority of the "Grenztruppen".

(c) Central Authority of the Security troops (Divisions and Brigades of the back areas).

(d) Central Authority of the Railway troops.

A constant watch was kept on the (a) Networks. They consisted of the communications between the Central Authority of the N.K.W.D. in MOSCOW and, the commanders of the Security troops working with the Army Groups, the directing staffs North and South, the less interesting independent GHQ Signals Regiments.

The messages were not readable.

Apart from the characteristics already noted they were also to be recognised by their use of Call-signs which were made up from a square

The actual Russian wireless station numbers were:

08-12 Central Authority MOSCOW.

3rd White Russian Front.
24 " " 2nd Baltic Front.
25 " " 1st White Russian Front.
26 " " 1st Ukraine Front.
27 " " 3rd " "
28 Higher directing Staff in LODZ.
29 Front Staff 4th Ukraine Front.
49 - 65. 1 - 17 Independent GHQ. Signals Regiments.
81 Directing Staff North (MINSK).
84 Front Staff 2nd Ukraine Front.
85 Directing Staff South.
87 Higher directing staff (?)Area East of STANISLAW.
80 Unidentified.

Method of working was controlled Kreis working. The Kreise were known by the number of the Controlling station. They were,

Kreis VIII Station 08 with 21,23,24 Night Frequency 3170/3380 Kcs.

Kreis IX " 09 with 20,21,25,28 Night Frequency 3850/4180 Kcs.

Kreis X " 10 with 81,85 Night Freq. 3950/4230 Kcs.

Kreis XI " 11 with 26,29,87 Night Freq.4580/4940 " Day Frequency 7400/8670 Kcs.

Kreis XII Station 12 with 27,84 Night Freq.4580/4940 Kcs.

Kreis LXXXI Station 81 with 20,21,22,23,24,25,28,49,50, 55,57, 59,60,61,63,65. Night Freq.2850/2975 Kcs. Day Frequency 4080/4480 Kcs.

Kreis LXXXV Station 85 with 26,27,29,51,52,53,54,56,58, 62,64,80,84,87. Night Freq. 2700/3050 Kcs. Day Frequency 3950/4400 Kcs.

2) Formation Networks consist of the communications between commanders of the security troops at Front Staffs and their regiments and between the latter and their battalions. Messages passed in these networks were for the most part readable.

On the front watched by us the following units were identified reading from South to North,

4th Ukraine Front 92, 30(?), (80?) and 215 "Grenztruppen" Regiments.
1st Ukraine Front 18, 88, and 333 "Grenztruppen" Regiments.

1st White Russian Front 127,157 and 38 " "

Call-sign Usage.

Call-signs were mostly pronouncable. The Front Staff networks usually changed their call-signs daily, the Regiment networks at regular intervals of several days, in many cases of weeks.

Frequencies used lay mainly between 2400 & 3600 Kcs.

It should be mentioned that 5-figure N.K.W.D. messages have been picked up in nets identified as belonging to the Army or the Air Force, such messages contained SMERSCH in the preamble. Such messages were originated by units of the Counter

transmit their messages.

The fourth group from the end of such messages had a special characteristic. The second bigram was the same as the first reversed and the fifth figure was a constant. Ex. 14412.

Networks in which such messages were sent were not to be regarded as N.K.W.D. networks

-- R E P O R T No. 29 --

N.K.W.D. - Codes.

by Obergefr. Georg THOMAS.(NAAS).

R4 Z C 1800 has since October 1943 had 50 pages, each consisting of 50 lines and totalling 2,500 clear groups, alphabetically arranged. Each page is shifted by means of "Chiffranten" and the bigrams (ab and cd) are then replaced by others according to substitution tables.

Shifting by means of Chiffranten enciphering: Any figure, chosen from Row A (sample code in Annexe 1), will indicate on any page, in Row B below, the figure which must be added to that standing beside the clear group (and subtracted when deciphering).

Substitution of bigrams: For the first and second halves of the 4-figure group (elements ab and cd) there are substitution tables, each of which contains 100 bigrams (each bigram, from 01 to 50 occurs twice). There are 10 such tables (numbered for the most part from 0 to 9). Sample below.

The reciphering is indicated by a 4-figure group (indicator) which appears at a definite position in the message and contains,

1) Number of the clear-group table (indicated with two digits)
2) Chiffrant
3) Number of the pagination table.

Example:

Indicator	0151
Chigruppe	2406.

Decipherment (according to tables below):

Element ab (=24) yields 20 according to the pagination table. The clear-group therefore is on page 20. Element cd yields 02 according to the clear-group table. From this the chiffrant is subtracted, in this case 1 (the number on page 20 under the fixed figure 5). Thus the clear group 2001 = Komandirowatj is derived.

R4 Z C 4 was used from 1933 (solved 1940) until 1942. There were 100 pages each with 100 clear groups arranged alphabetically. Recipherment by means of 31 substitution tables.

Bigram substitution table for RH Z C 1800.

(For deciphering; for enciphering tables, the encipher version of the same table is used.)

	0	1	2	3	4	5	6	7	8	9
0	49	37	50	21	13	36	02	10	18	16
1	47	22	31	-	-	-	-	-	-	etc.
2										
3										
4										
5										
6										
7										
8										
9										

Clear group table
No.1
(for element cd)

	0	1	2	3	4	5	6	7	8	9
0										
1								18	49	9
2	15	28	37	50	20	25	07	11	etc	
3										
4										
5										
6										
7										
8										
9										

Pagination table No.1
(for element ab)

VI AIR FORCE TRAFFICS

-- REPORT No. 30 --

Study of Russian Air Force Traffics,

"Bearbeitung von Luftwaffenverkehren",

by Lt. Edward WOELLNER (NAAS).

Air traffic was, in principle, not covered, and cover was dropped by the Companies as soon as a traffic was recognised as Air. For this purpose, data on Air as well as Army traffic had to be kept in the card indexes. These statistics included such as were derived from air traffic taken "by mistake"; also data supplied by the G.A.F. Sigint. Abteilungen III/353 (Luftflotte 4) and II/353 (Luftflotte 6), which were passed on by the NAAS to the Long Range Sigint. Companies. The Companies kept air data in the Army card index, but the NAAS had special indexes (similar to the Army indexes). NAAS had a section "Air Force".

The "Air Force" section of NAAS had the following tasks:

1) Collection of "Air Force" data; passing of such data to the Long Range Sigint. Companies.

2) Interpretation of Air traffic not recognised as Air by the Companies.

3) Forwarding of new Air traffic picked up in search to the competent G.A.F. Sigint. Abteilung.

4) Passing of particularly interesting messages to the G.A.F. Sigint. Abteilungen.

5) Exploitation of Air signals indicating intentions and battle order of Army formations.

6) Compilation of the "Air" section of the (Army) Sigint. Sitrep. (based on reports of the G.A.F. Sigint. Abteilungen and our own material).

In some exceptional cases, G.A.F. traffic was also expressly covered:

(a) When signals links to the G.A.F. Sigint. Abteilung, for example, were cut. During such a period we recognised concentrations and movements on the 1st Ukrainian Front from cover of I Guards Ground Attack Air Corps.

(b) During large-scale operations, the routes of advance of armoured Corps were worked out from signals in Air nets.